

Extended calculations of a special Harmonic number

John Blythe Dobson (j.dobson@uwinnipeg.ca)

February 25, 2014

Abstract

The search for values of p for which the Harmonic numbers $H_{\lfloor p/6 \rfloor}$ vanish mod p , carried to $p < 600,000$ by Schwindt [6] in 1983, is extended here to $p < 12,000,000,000$, and two new solutions are reported.

Keywords: Harmonic numbers, Fermat quotient, Fermat's Last Theorem

In 1983 Schwindt [6] sought solutions of the Harmonic number congruence

$$H_{\lfloor p/6 \rfloor} := \sum_{j=1}^{\lfloor p/6 \rfloor} \frac{1}{j} \equiv 0 \pmod{p}, \quad (1)$$

with $\lfloor \cdot \rfloor$ denoting the greatest-integer function, and found the single case $p = 61$ with $p < 600,000$. The three zeros found by us, with $p < 12,000,000,000$, are:

$$61, 1\,680\,023, 7\,308\,036\,881.$$

We know of no intervening computations of these numbers *per se*, though as we afterwards learned, our solutions had already appeared in another guise, as will be explained below. The historical motivation for the study of this sum is the famous proof given by Emma Lehmer in 1938 ([4], p. 358) that (1) is a necessary condition on the exponent p for the failure of the first case of Fermat's Last Theorem (FLT). This result retains its interest despite the full proof of FLT by Andrew Wiles. A survey of related results appears in [5], and subsequent progress in this direction has been made in [7] and [1]. It should however be noted that a statement in [1], pp. 389–390, implying that $H_{\lfloor p/N \rfloor} \equiv 0 \pmod{p}$ has a solution $p < 2,000$ for every N between 2 and 46 other than 5, is incorrect (at least if we require $p > N$ to ensure that the sum is not vacuous). In fact, we have determined that there are no solutions with $p < 3,750,000$ for $N = 5, 12, 13, 17, 18, 20, 29, 30, 31, 43$.

Schwindt reports obtaining the right-hand side of (1) by direct evaluation, and states that this operation constituted nearly half the work for a project described as having been “run at night over half a year.” As he cites Lehmer's work, it is not clear why he chose to perform the calculations in such a processing-intensive manner, rather than to exploit her result that

$$H_{\lfloor p/6 \rfloor} \equiv -2 \cdot q_p(2) - \frac{3}{2} \cdot q_p(3) \pmod{p}, \quad (2)$$

where the $q_p(b) := (b^{p-1} - 1)/p$ are Fermat quotients. On Schwindt's own showing, his method has an algorithmic complexity of order $p \log p$, because the calculation of each modular inverse has order $\log p$, while the range over which they must be summed has order p . In contrast, the complexity of each of the Fermat quotients in (2) has only order $\log p$, the same as that of a single modular inverse, and it is only necessary to calculate two of them. (In fact, as will be shown below, it is possible to treat the two together; and the ensuing analysis assumes this saving.) In other words, over a range of p running from some small number ϵ to n , the processing of Schwindt's calculations would have order

$$\int_{\epsilon}^n x \log x \, dx \sim \frac{n^2}{2} \left(\log n - \frac{1}{2} \right),$$

while that for the right-hand side of (2) would have only order

$$\int_{\epsilon}^n \log x \, dx \sim n(\log n - 1),$$

and the results of our tests are in close agreement with these predictions. These models fail to take into account the diminishing frequency of the primes as n increases and thus are not fully realistic, but asymptotically the effect of any further refinement would be dwarfed by the fundamental differences between the two methods.

In Table 1 below, we give a comparison of running times for the Fermat-quotient method versus that of Schwindt, for various upper limits n : 600,000 (the limit of Schwindt's calculations), 1,680,023 (the first large zero), and 7,308,036,881 (the second large zero). The last limit is attainable only in the case of the Fermat-quotient test, not Schwindt's. These calculations were performed in Mathematica on a typical desktop computer, with a 3.2 GHz processor and 4 GB of memory, with the network connection disabled to prevent interruptions. Each run was begun at the number 7 (the least prime for which $H_{\lfloor p/6 \rfloor}$ is meaningfully defined) and extended precisely to the stated value of the limit n . Though running times inevitably vary over the course of multiple trials, these were performed under consistent conditions and may be assumed to give a good relative sense of the times involved, so we have reported them precisely as obtained, rounded to the nearest second.

These results suggest that Schwindt's calculations up to the limit $n = 600\,000$ could not have been profitably pursued much further using the equipment then available. Indeed, even with today's processing capabilities, such calculations could only be extended about a hundredfold. It would be inconceivable to find the third zero using Schwindt's test in its obvious form, as the estimated runtime is about 10,000 years; but this objection is almost moot because even an attempt to spot-check this solution by Schwindt's method produces a memory allocation

failure error in Mathematica. In contrast, the Fermat-quotient test obtains the result in about 39,864 seconds (just over 11 hours).

We shall now describe how the calculation based on Emma Lehmer's congruence (2) was optimized. Because we are only interested in locating its zeros and do not require the actual values, we are free to disregard sign and scale, and may multiply throughout by -2 to clear the negative signs and the fraction, establishing that for $p > 5$ the zeros coincide with those of

$$4 \cdot q_p(2) + 3 \cdot q_p(3).$$

Applying in reverse the logarithmic and factorization rules for the Fermat quotient given by Eisenstein [2], this expression may be realized more compactly as follows:

$$q_p(2^4) + q_p(3^3) \equiv q_p(2^4 \cdot 3^3) \equiv q_p(432) \pmod{p} \quad (p > 5).$$

By simplification and consolidation of the Fermat quotient calculation, we are able to improve the running time considerably. Moreover, this device alerted us to the fact that pertinent prior literature might include studies of the divisibility of the Fermat quotient by p for composite bases, and such a study was indeed located in the form of Fischer [3], which treats the base 432. Disregarding his first solution $p = 5$, which is too small to qualify as a solution to Schwindt's problem, our results are in perfect agreement with his so far as they overlap. And because Fischer has carried his work to the enormous limit of $p < 48\,000\,000\,000\,000$ without finding further solutions, it became clear that it would be pointless for us to continue our search further. Fischer's limit is more than five orders of magnitude higher than any calculation for $H_{\lfloor p/6 \rfloor}$ that could be achieved by direct calculations of sums of reciprocals in under a decade of processing time.

A survey of the literature, and the evidence of our own calculations of $H_{\lfloor p/N \rfloor}$ for an as-yet unpublished project, suggest that the zero 7 308 036 881 with $N = 6$ is the largest presently known for any value of $N < 46$ (a limit chosen to coincide with results in the important study by Dilcher & Skula [1]). Zeros for larger values of N are of less interest because then $H_{\lfloor p/N \rfloor}$ is less likely to have any demonstrable connection with FLT, or to have a known evaluation in terms of the Fermat quotient, the Fibonacci quotient, or other interesting object.

Table 1: Comparison of timings for calculations of zeros of $H_{\lfloor p/6 \rfloor}$ by various methods

upper limit n	Fermat-quotient test	Schwindt's method
600,000	2 seconds	1,633 seconds
1,680,023	5 seconds	12,422 seconds
7,308,036,881	39,864 seconds	(impossible)

References

- [1] Karl Dilcher & Ladislav Skula, “A new criterion for the first case of Fermat’s Last Theorem,” *Math. Comp.* **64** (1995) 363–392.
- [2] [G.] Eisenstein, “Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definirt werden,” *Berichte Königl. Preuß. Akad. Wiss. Berlin* **15** (1850) 36–42.
- [3] Richard Fischer, “Fermatquotient $b^{(p-1)} \equiv 1 \pmod{p^2}$,” available online at http://www.fermatquotient.com/FermatQuotienten/FermQ_Sort.
- [4] Emma Lehmer. “On Congruences involving Bernoulli numbers and the quotients of Fermat and Wilson,” *Ann. of Math.* **39** (1938) 350–360.
- [5] Paulo Ribenboim, *13 Lectures on Fermat’s Last Theorem*. New York, etc.: Springer, 1979.
- [6] H. Schwindt, “Three summation criteria for Fermat’s Last Theorem,” *Math. Comp.* **40** (1983) 715–716.
- [7] Zhi-Hong Sun & Zhi-Wei Sun, “Fibonacci numbers and Fermat’s Last Theorem,” *Acta Arith.* **60** (1992) 371–388.